In the Abstract:

ABSTRACT OF THE DISCLOSURE

~~ZERO KNOWLEDGE PROOF CRYPTOGRAPHIC METHODS AND DEVICES~~

~~The invention relates to a~~ A cryptography method involving a keyholder having a number $m \geq 1$ of private keys $Q_1, Q_2, ..., Q_m$ and respective public keys $G_1, G_2, ..., G_m$, each pair of keys (Q_i, G_i) (where $i = 1, ..., m$) satisfying either the relationship $G_i = Q_i^v \bmod n$ or the relationship $G_i \times Q_i^v = 1 \bmod n$, where n is a public integer equal to the product of f (where $f > 1$) private prime factors $p_1, ..., p_f$, at least two of which are separate, and the exponent v is a public integer equal to a power of 2. ~~The invention teaches among other things~~ Disclosed is what mathematical structure may be imparted to the public keys for it to be impossible to calculate said private keys from said public parameters in a reasonable time unless said prime factors are known. ~~The invention also relates to devices~~ Devices adapted to implement the method are also disclosed.